Obtaining Visual Environmental Data Through Modification of Native LED Monitor Behavior

25 November 2024
Simon Edwards
Research Acceleration Initiative

Introduction

Although some studies have demonstrated that LASER light may be used, under very specific circumstances, to inject data into certain devices such as Xerox machines provided access to the LED display on the Xerox machine itself, the possibility of converting things such as LED computer monitors into visual surveillance devices through firmware tampering has not been properly explored.

Abstract

Provided that a virus can be delivered to the computer into which a target LED monitor is connected, the native behavior of the monitor as well as the graphics driver can be used in conjunction with one another in order to allow for indirect measurement of the intensity of ambient light striking each LED node in order to ultimately build a crude image of the environment in front of the monitor. Although the directionality of light which can be captured is relatively narrow, this would not be problematic if in cases wherein the objective is facial recognition of a user of a system. For example, a high-value target in the Middle East whose facial characteristics are known could be located by converting all of the LED monitors in the region into covert facial recognition scanners.

A given node of an LED display may be converted into a light-measuring device when the device is ‘on’ by first increasing the refresh rate of the display beyond the rated maximum so that pixels will attempt to change color at the maximum rate physically achievable. The precise maximum will vary from one node/pixel to the next depending upon manufacturing irregularities. However, even the baseline refresh rate could be expected to change for any given pixel on the basis of the influence of ambient light. The more intense the ambient light, the greater a latency in actual refresh rates (relative to baseline) could be expected.

The next element required would be a mechanism for assessing the rate at which a given pixel’s color changes (in Hertz) compared to baseline. Via control over the graphics driver output, an LED display may be made to switch to a black screen for 1/60th of one second and then to pure white for 1/60th of one second. This may be done for the whole of the display or for subsections of the display, one after the next, in order to progressively build a map of the ambient light from the perspective of various relative positions on the monitor’s surface.

As there is no self-diagnostic for refresh rates of individual pixels built into LED monitors, a proxy method must be utilized.

When an LED monitor switches from displaying a darker overall image to a brighter overall image, there is increased RF interference from the individual LED lights. This increase is measurable by radio detector, even for extremely small pixels. As virtually all computers are equipped with Bluetooth and WiFi antennae, these antennae can be exploited in order to measure subtle changes in the EM environment associated with LED light activation.

By measuring with high precision the length of time required for a given pixel to change from zero brightness to full brightness and comparing that value to a baseline value, an estimate of the brightness of ambient light can be made, provided, of course, access to the Bluetooth antenna, to the graphics driver and to the firmware of the monitor so as to enable limits on refresh rate to be temporarily lifted.

By repeating this process for each pixel or node, a crude visual representation of the face of the individual sitting behind the screen can be constructed through extrapolation.

Conclusion

The ability to convert an ordinary LED monitor into a camera constitutes a potent intelligence-gathering capability deserving of further development.